Journal of Health & Biomedical Law, Vol. V (2009): 1-32

Suffolk University Law School

What's Wrong With Health Privacy?*

Nicolas P. Terry**

I. Introduction

In 2000, President Clinton introduced the landmark Standards for Privacy of Individually Identifiable Health Information[1] (federal standards) with the words "[n]othing is more private than someone's medical or psychiatric records."[2] It is well known that the *Health Insurance Portability and Accountability Act of 1996* (HIPAA)[3] committed the federal government to a process of "Administrative Simplification" to reduce healthcare costs, but Congress wanted to limit how far the healthcare industry could externalize attendant privacy risks to patients.[4] Yet, in the aftermath, what should have been a substantial victory for patient autonomy and informational privacy has morphed into yet another divisive debate about professionalism and healthcare regulation. State and federal privacy law may be omnipresent, the pages of medical journals and law reviews may be filled with exhortations of confidentiality, and the media, often disingenuously, may be quick to pounce on system failures, but health information privacy is surprisingly fragile.

 This essay is an updated version of a chapter (by the same name) that originally appeared in LEGAL PERSPECTIVES IN BIOETHICS, 68-94 (Ana S. Iltis et al. eds., 2008).

** Chester A. Myers Professor of Law, Senior Associate Dean for Faculty, Professor of Health Management & Policy, Saint Louis University, email: terry@slu.edu. I thank Kathy Cerminara, Tim Greaney, Trevor Wear, and Brian Bohnenkamp for their helpful comments on the original chapter. I thank Jessica Flinn, my current research assistant, for her help in updating this version.

[1] 45 C.F.R. §§ 160, 164 (2009).

[2] Press Release, The White House, Office of the Press Sec'y, Remarks by the President on Medical Privacy (Dec. 20, 2000), http://www.hhs.gov/ocr/privacy/hipaa/news/whpress.html (last visited Jan. 22, 2009).

[3] Health Insurance Portability and Accountability Act of 1996, Pub. L No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C., 42 U.S.C. and 18 U.S.C.).

[4] 42 U.S.C. § 1320d-2(d)(2) (2006) (instituting safeguards to protect patient information).

Elsewhere, I have argued that the necessity of protecting the privacy of health information is broadly, if not universally, accepted (at least in the ethical and legal domains), yet counter-intuitively dogged by controversy.[5] Rather than an accepted social imperative protected by a powerful triumvirate of ethical constraints, effective laws, and operational necessities, I see a construct that lacks consistent terminology, a convincing rationale, or general principles that can be effectively conveyed to patients and providers.

This essay seeks to identify some of the reasons why "privacy" remains so contentious. Here I suggest several possible answers ranging from "micro" issues such as what we understand by health privacy, to more "macro" and operational issues encountered as we seek to protect health information. First, lawyers have made consistent errors in the terminology applied to the protection of medical privacy; second, both the legal and ethical domains have failed to apply a consistent and robust rationale for health privacy, leaving it prey to consequentialist thought and policy; third, the declining importance of the physician–patient relationship as the touchstone for obligations, particularly confidentiality, has created a "rights" vacuum; fourth, the health information revolution truly is revolutionary in its reach and its concomitant threats to privacy and confidentiality; and, finally, as privacy regulation increasingly lies in the sphere of governmental command-control regulation, it has joined the list of targets in the professionalism-market-regulation conflict over millennial healthcare delivery.

II. Errors in Terminology

Upon initial analysis, the legal and ethical domains display a degree of synchronization regarding the protection of patient data. However, as discussed below, their prevailing rationales either diverge or are used inconsistently.[6] As described in this section, both domains commit errors in their terminology and their operational approaches.

In the ethical domain Tom L. Beauchamp and James F. Childress describe a patient's right of privacy that is not limited to information about the person but extends to "zones of intimacy, secrecy, anonymity, seclusion, or solitude."[7] Similar observations

---

[5] Nicolas P. Terry, *Privacy and the Health Information Domain: Properties, Models and Unintended Results*, 10 EUR. J. HEALTH L. 223, 223 (2003) [hereinafter *Health Information Domain*] (identifying and exploring three reasons for controversy surrounding protecting privacy of health information).

[6] TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 410 (4th ed., 1994).

[7] *Id.* at 408. This is reflected in AMERICAN MEDICAL ASSOCIATION, COUNCIL ON ETHICAL AND

populate the legal domain. However, unpacking the legal notion of privacy yields a picture that is both incoherent and incomplete, suggesting not only terminological flaws but also a considerable disconnect between ethical and legal constructs, a disconnect that seems heightened when we examine the protection of health information.

Legal and regulatory systems may potentially utilize three basic models for the protection of personal information: deidentification, collection control, and disclosure control. The first of these models assumes (more or less correctly[8]) that data that is deidentified prior to collection (or, somewhat less successfully, prior to disclosure) reduces or eliminates personal risks associated with its use or processing.[9] The second potential protective model is to place limitations on data collection. Such a model could, for example, prohibit all collection in certain circumstances (e.g., the harvesting of genetic information by life insurers) or limit collection via a proportionality rule (e.g., only information necessary for the purposes of treatment). The third protective model, again primarily focusing on informational privacy, is to place limitations on data disclosure (e.g., hospital records may be disclosed to physicians but not drug companies).

Oddly, our legal systems are only dimly cognizant of the deidentification model. For example, while the federal standards are generally inapplicable to deidentified health information,[10] they do not require deidentification.[11] Even more surprisingly, the U.S.

JUDICIAL AFFAIRS, PRIVACY IN THE CONTEXT OF HEALTH CARE (2001), http://www.ama-assn.org/ama1/pub/upload/mm/369/ceja_2i01.pdf (last visited Jan. 18, 2008):

> Physicians must seek to protect patient privacy in all of its forms, including (1) physical, which focuses on individuals and their personal spaces, (2) informational, which involves specific personal data, (3) decisional, which focuses on personal choices, and (4) associational, which refers to family or other intimate relations. Such respect for patient privacy is a fundamental expression of patient autonomy and is a prerequisite to building the trust that is at the core of the patient–physician relationship.

[8] The greatest challenge to the deidentification model is the growing impossibility of deidentification because of, for example, the unique genetic signature of data, or the exposure of apparently deidentified data to reidentification because of, for example, geo-coding. *See, e.g.*, Gerard Rushton et al., *Geocoding in cancer research: a review*, 30 AM. J. PREVENTIVE MED. S16, S19-20 (2006) (discussing potential privacy dilemmas in geocoding in relation to cancer research).

[9] Questions persist about the level of identifier-stripping necessary to create deidentified data. For example, data that has been only "anonymized" has not been deidentified.

[10] 45 C.F.R § 164.514(a) (2009) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.").

legal domain recognizes few collection-centric rules. For example, the Restatement's black-letter law of "privacy" provides as follows:

> The right of privacy is invaded by
>
> (a) unreasonable intrusion upon the seclusion of another . . . or
>
> (b) appropriation of the other's name or likeness . . . or
>
> (c) unreasonable publicity given to the other's private life . . . or
>
> (d) publicity that unreasonably places the other in a false light before the public.[12]

This "right of privacy" promises far more than it delivers. On its face the Restatement fails to provide any general or comprehensive "right of privacy." It is no more than a listing of modest protections – nominate and discrete tort actions applicable in a narrow range of circumstances rather than fact-sensitive applications of a general principle or theory of privacy. Further, even a cursory examination of this "right of privacy," as it applies to health providers, suggests that only the protection against "unreasonable intrusion upon the seclusion of another" is in any way applicable.

This seclusion-based privacy model has seldom been applied to the health domain and its doctrinal elements limit its applicability to outlying cases. A commonly cited example of health privacy protection is *Estate of Berthiaume v. Pratt*,[13] where a physician was held to have intruded into a dying cancer patient's "physical or mental solitude or seclusion" when he took photographs against the patient's wishes. But, even where the doctrine is generally applicable to a particular circumstance, the doctrine is quite restrictive. Thus, in *Knight v. Penobscot Bay Medical Center*,[14] a nurse's husband arrived at a hospital to pick up his wife. To give him something to do while he waited, the

---

[11] In contrast, for example, European law requires that cell phone customers be allowed to request non-itemized billing and requires providers to make data that it collects regarding a user's location anonymous. Parliament and Council Directive 2002/58/EC, art. 7, 9, 2002 O.J. (L 201) 37, 41, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20060-503:EN:PDF (last visited Dec. 13, 2008) (concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)).

[12] Restatement (Second) of Torts § 652A(2) (1977).

[13] 365 A.2d 792 (Me. 1976).

[14] 420 A.2d 915 (Me. 1980).

husband was gowned and permitted to observe a stranger's labor and delivery. The plaintiff's cause of action failed because there was no evidence that the husband had intended the intrusion into the patient's seclusion. Only in extreme cases will privacy, as understood by the legal system, have an impact on patient health information. For example, in *Swarthout v. Mutual Service Life Insurance*,[15] the court held that the doctrine could apply when a life insurance company altered an applicant's medical information release, used it to obtain information from other sources, and transmitted the information to a medical-records database, which was available to other insurers.

In contrast to deidentification and collection, the third protective model, whereby limitations are placed on data disclosure, is well established in U.S. normative circles. For example, in the ethical domain, the American Medical Association (AMA) states that "[t]he physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest."[16] Although frequently described in terms of "privacy" and "privacy law," the legal protections applied to patient health information by the common law, state statutes, or the federal standards have very little to do with either. Aside from a few "intrusion upon the seclusion" actions, the modern law of health privacy resides in the far narrower, disclosure-centric model doctrinally captured in cases, statutes, and regulations dealing with breach of confidence. A patient exercises his right of privacy (as recognized by the ethical domain) when he chooses to provide information to his physician (albeit a "right" that is illusory if it is a condition of treatment). Thereafter, dissemination of that information by the physician is limited by ethical and legal standards of confidence,[17] hereinafter referred to as confidentiality. Today, when courts and regulators speak of medical "privacy" they are usually in error, mislabeling what are obligations of "confidentiality."

Long before the promulgation of the federal standards, most states had developed common law[18] and statutory protections applicable to health information.[19]

---

[15] 632 N.W.2d 741 (Minn. Ct. App. 2001).

[16] AMERICAN MEDICAL ASSOCIATION, COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS, FUNDAMENTAL ELEMENTS OF THE PATIENT–PHYSICIAN RELATIONSHIP para. 4 (1990), www.ama-assn.org/ama1/pub/upload/mm/369/ceja_aa90.pdf (last visited Jan. 18, 2008) [hereinafter FUNDAMENTAL ELEMENTS].

[17] BEAUCHAMP & CHILDRESS, *supra* note 6, at 410. It may also be limited by express agreement between the parties.

[18] *See, e.g.,* Givens v. Mullikin *ex rel.* Estate of McElwaney, 75 S.W.3d 383 (Tenn. 2002); Berger v. Sonneland, 26 P.3d 257 (Wash. 2001); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 522 (Ohio

Languidly, the courts articulated a cause of action for breach of confidence. Decisions explained the distinction between defendants in privacy and confidence actions—"Only one who holds information in confidence can be charged with a breach of confidence. If an act qualifies as a tortious invasion of privacy, it theoretically could be committed by anyone."[20] Further decisions have clarified the differences between the types of data at issue in privacy and confidence proceedings: "Not every secret concerns personal or private information; commercial secrets are not personal, and governmental secrets are neither personal nor private. Secrecy involves intentional concealment. 'But privacy need not hide; and secrecy hides far more than what is private."[21]

The development of the common law of confidentiality has been "distinguished" by quite arcane discussions as to the correct doctrinal basis for protecting patient confidences (including implied contract, breach of a fiduciary relationship, and even "privacy"). Only in the last decade could it be said that "[s]lowly and unevenly, through various gradations of evolution, courts . . . moved toward the inevitable realization that an action for breach of confidence should stand in its own right, and increasingly courts have begun to adopt it as an independent tort in their respective jurisdictions."[22]

Generally, state statutory models have been more successful in reflecting the realities of modern healthcare delivery and the particular issues posed by informational privacy. Although still generally limited to a collection-centric approach (and frequently

---

1999) (assessing liability on doctors for unauthorized disclosure of patient information); Alberts v. Devine, 479 N.E.2d 113, 119 (Mass. 1985) (determining physicians have duty not to disclose information unless serious danger to patient or others); Humphers v. First Interstate Bank of Or., 696 P.2d 527, 533 (Or. 1985) (recognizing importance of right of privacy but not applicable to this case); Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 337 (N.Y. Sup. Ct. 2001) (holding pharmacists have a fiduciary duty not to disclose confidential health information); Hurvitz v. Hoefflin, 101 Cal. Rptr. 2d 558, 561 (Cal. Ct. App. 2000) (determining unconstitutional to seal documents); Jeffrey H. v. Imai, Tadlock & Keeney, 101 Cal. Rptr. 2d 916 (Cal. Ct. App. 2000) (recognizing zone of privacy of California Constitution to extend to one's medical records); McCormick v. England, 494 S.E.2d 431, 434 (S.C. Ct. App. 1997) (acknowledging common law tort action for breach of confidence).

[19] *See, e.g.,* CAL. CIV. CODE §§ 56–56.37 (West 2007) (requiring patients' information to remain confidential); 2001 Haw. Sess. Laws 244; MONT. CODE ANN. §§ 50-16-501 to 16-553 (2007) (recognizing importance of confidentiality in patient information); WASH. REV. CODE ANN. §§ 70.02.005 to .02.904 (West 2003) (providing for protection of patient information); WIS. STAT. § 146.83 (2001) (discussing release and transfer of patient information).

[20] *Humphers*, 696 P.2d at 530.

[21] *Id.* at 529.

[22] Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999).

mislabeled as going to privacy rather than confidentiality), these statutes have tended to be more comprehensive and coherent than their common law progenitors. Such statutes frequently are more explicit in extending the duty of confidence to the myriad of providers and insurers involved in modern healthcare delivery. For example, by requiring written authorization for disclosure and making access available to the courts, law enforcement, and public health entities.[23] These state "privacy" statutes, however, have not supplanted the common law action for breach of confidence, primarily because most statutes do not permit a private right of action by patients.[24]

The federal standards apply to a broad range of "covered entities"[25] including, for example, health, but not life, insurers. These providers,[26] such as hospitals, physicians, and health plans, are subject to the regulations if they transmit health information "in electronic form in connection with a [HIPAA–EDI transaction]."[27] The federal standards place limitations on the disclosure of "protected health information,"[28] including information that "relates to the past, present, or future physical or mental health or condition of an individual"[29] and identifies or could identify the individual.[30] Thereafter, the provider may only disclose private health information (PHI) as permitted by the federal standards.[31]

Unlike the situation at common law, the federal standards do not give patients a private right of action for unauthorized disclosures. Rather, enforcement of the disclosure rules is accomplished with a compliance model, detailing the appointment of a "privacy officer," the incorporation of staff training,[32] and the development and disclosure of "privacy" policies, all, generally, through complex regulatory oversight.[33]

---

[23] *See, e.g.*, CAL. CIV. CODE § 56.10 (West 2009).

[24] A small number of state statutes do allow such an action. *See, e.g.* WIS. STAT. § 146.84 (1)(c) (2001) ("An individual may bring an action to enjoin any violation of § 146.82 or 146.83 or to compel compliance with § 146.82 or 146.83 and may, in the same action on, seek damages as provided in this subsection."). *See also* CAL. CIV. CODE § 56.35 (West 2009) (allowing recovering of compensatory and punitive damages as well as attorneys' fees when medical information has been disclosed in violation of law); 2001 Haw. Sess. Laws 244.

[25] 45 C.F.R. § 164.502(1) (2009).

[26] *See* 45 C.F.R. § 160.103 (2009) (defining providers).

[27] 45 C.F.R. § 160.102(a)(3) (2009). For a discussion of HIPAA–EDI transactions see *infra*, text accompanying note 93 *et seq.*

[28] *See* 45 C.F.R. § 164.501 (2009).

[29] 45 C.F.R. § 160.103 (2009).

[30] 45 C.F.R. § 164.501 (2009).

[31] *See* 45 C.F.R. § 164.502(a) (2009).

[32] *See* 45 C.F.R. § 164.530 (2009).

[33] *See* 45 C.F.R. §§ 160.300 to .312 (2009).

For providers, therefore, the federal "privacy" experience owes little to the general principles of confidentiality recognized in the ethical domain and moves closer to other "hated" oversight models such as those applying to patient dumping,[34] reimbursement, or fraud and abuse.[35] This is a theme that I return to below.[36]

III. An Inadequate "Privacy-Confidence" Rationale

In the ethical domain, the most cogent justification for privacy and confidentiality is the principle of autonomy. For example, Beauchamp and Childress argue that claims to privacy "are justified by rights of autonomous choice that are correlative to the obligations expressed in the principle of respect for autonomy."[37] As already noted, in the information domain a patient exercises this autonomy-based right of privacy when he or she shares information with his or her physician and thereafter relies on ethical or legal standards of confidentiality to police subsequent disclosure.[38] It is arguable that today's health confidence laws (particularly the federal standards) do not reference any underlying autonomy model. Rather, they are based on more limited and less satisfying instrumental models and, worse, are increasingly justified on utilitarian constructs (specifically, "rule" Utilitarianism).[39]

Of course, the autonomy rationale for privacy and confidentiality is not universally accepted, and the two principles have had their share of consequentialist and instrumentalist rationales.[40] Even Jay Katz's seminal account of patient autonomy admits that the "right to privacy – the right to keep one's thoughts and feelings to oneself"[41] must "bend to psychological autonomy"[42] so as to further autonomy's central goal of "respectful conversation."[43] Equally, Charles Fried's conception of privacy – "[t]o respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at he heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as

---

[34] *See, e.g.*, Emergency Medical Treatment and Active Labor Act, 42 U.S.C. § 1395dd (2006).

[35] *See, e.g.*, Medicare & Medicaid Anti-Kickback Statute, 42 U.S.C. § 1320a-7b(b); Ethics in Patient Referrals Act (STARK), 42 U.S.C. § 1395nn (2006).

[36] *See infra* text accompanying note 116, *et seq.* (discussing managing privacy in health information domain).

[37] BEAUCHAMP & CHILDRESS, *supra* note 6, at 410.

[38] *See supra* note 17 and accompanying text.

[39] BEAUCHAMP & CHILDRESS at 409–10.

[40] *Id.* at 409–24.

[41] JAY KATZ, THE SILENT WORLD OF DOCTOR AND PATIENT 127 (1984).

[42] *Id.* at 128.

[43] *Id.* at 141–42.

oxygen is for combustion"[44] – on which he bases a robust critique of instrumental (and primarily utilitarian) justifications for privacy is itself somewhat instrumentalist when it argues that "privacy is not just one possible means among others to insure some other value, but that it is necessarily related to ends and relations of the most fundamental sort; respect, love, friendship and trust."[45]

Instrumental justifications for medical privacy and confidentiality are simply stated. Thus, patients provide information to physicians in the belief that it will further their diagnosis and treatment while physicians respect confidences in order to encourage patients to disclose personal and medical information that will make diagnosis and treatment more effective. This justification may not be an entirely flawed way of looking at the physician-patient discourse. However, it is a notion that stumbles outside of the physician–patient paradigm and becomes unstable when applied in, for example, institutional or industrial models of care. In such models, the notion falls prey to modern utilitarian arguments that see the generation, dispersal, and processing of longitudinal patient health information primarily as a necessity to reduce overall healthcare costs and to minimize medical error. As the context changes, therefore, the simple and probably innocuous instrumental approach becomes increasingly utilitarian.

The current tensions in the medical privacy-confidentiality debate are somewhat reminiscent of familiar debates about the nature of informed consent. As described by Beauchamp and Childress, there is a vector between two senses of informed consent. In the first sense, "[a]n informed consent is an *autonomous authorization* by individuals of a medical intervention or of involvement in research."[46] In the second sense, consent is "analyzable in terms of *the social rules of consent* in the institutions that must obtain legally valid consent from patients or subjects before proceeding with therapeutic procedures or research."[47] Consider, in this context, Braddock's view that informed consent primarily rotates around social rules, specifically legal notions:

> [T]he well-known mnemonic PAR reminds the clinician to disclose the nature of the procedure, alternatives, and risks in any informed consent discussion. The rationale of this approach either satisfies an administrative requirement or protects oneself from liability, rather than view-

---

[44] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968), *reprinted in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 205 (Ferdinand D. Schoeman ed., Cambridge University Press 1984).

[45] *Id.*

[46] BEAUCHAMP & CHILDRESS, *supra* note 6, at 143.

[47] *Id.* at 144.

> ing the decision making process as a meaningful path toward fostering patient involvement.[48]

Braddock's observations capture a serious disconnect between the ethical and (common law and statutory) regulatory approaches to informed consent. Beauchamp and Childress may argue, "from the moral viewpoint, informed consent has less to do with the liability of professionals . . . and more to do with the autonomous choices of patients and subjects."[49] Yet, ethical and legal domains continue to grow apart, increasing the vector between the autonomy rationale and social rules informed by legal rules and day-to-day operations. Informed consent law tends to focus on the narrow issue of "consent" rather than the disclosure of information that increases patient choice and participation. Only a few jurisdictions have recognized a broader approach, such as expanding the doctrine's reach to include all treatment risks[50] and other information such as non-medical risks[51] risks of non-treatment,[52] and physician impairments.[53] Today, courts are far more likely to limit the duty to disclose to cases involving surgical risks.[54] In contrast, ethical observations on disclosure[55] or "choice"[56] are far more

---

[48] Clarence H. Braddock, III et al., *Informed Decision Making in Outpatient Practice: Time to Get Back to Basics,* 282 J. AM. MED. ASS'N 2313, 2313–14 (1999).

[49] BEAUCHAMP & CHILDRESS, *supra* note 6, at 146.

[50] *See, e.g.*, Matthies v. Mastromonaco, 733 A.2d 456, 464 (N.J. 1999):

> It is not dispositive that the alternative that the physician recommends is more or less invasive than other alternatives. (citation omitted) The critical consideration is not the invasiveness of the procedure, but the patient's need for information to make a reasonable decision about the appropriate course of medical treatment, whether invasive or noninvasive.

[51] *See, e.g.*, Arato v. Avedon, 858 P.2d 598, 599–600 (Cal. 1993) (declining to require mandatory disclosure of life expectancy in case where physician allegedly failed to discuss the low life expectancy of a patient suffering from pancreatic cancer).

[52] *See, e.g.*, Truman v. Thomas, 611 P.2d 902, 907 (Cal. 1980) (holding that physician had a duty to provide the decedent with all information material to her decision whether or not to undergo pap smear diagnostic test). *Cf.* Vandi v. Permanente Med. Group, Inc., 9 Cal. Rptr. 2d 463, 467 (Cal. Ct. App. 1992) (holding that the duty of disclosure is predicated upon a recommended treatment or diagnostic procedure and the failure to recommend a procedure must be addressed under ordinary medical negligence standards).

[53] *See, e.g.*, Johnson by Adler v. Kokemoor, 545 N.W.2d 495, 498 (Wis. 1996) (determining physician needed to inform patient on his experience, comparative risk statistics, and availability of other, better centers and physicians).

[54] *See, e.g.*, Morgan v. MacPhail, 704 A.2d 617, 618 (Pa. 1997) (holding that informed consent was not required in cases involving non-surgical procedures); *see also* Duttry v. Patterson, 771 A.2d 1255, 1259 (Pa. 2001) ("[I]he doctrine of informed consent is not the legal panacea for all damages arising out of any type of malfeasance by a physician.").

nuanced yet far truer to the autonomy rationale.

A similar vector can be detected in the medical confidentiality debate. The common law originally eschewed a rights-based approach, preferring to view breach of confidence as based on fidelity or implicit agreement. In contrast, the movement towards tort-based recovery for breach of confidence, an action recognized by a growing number of jurisdictions,[57] is clearly more rights-based and reminiscent of some of the early autonomy-based informed consent decisions.[58] Consider the frame established in one of the more influential common law confidentiality cases:

> [T]here is widespread public knowledge of the ethical standards of the medical profession and widespread belief that confidences made by a patient to a physician may not be disclosed without the permission of the patient. Patients . . . have the right to rely on this common understanding of the ethical requirements which have been placed on the medical profession and to obtain damages against a physician if he violates such confidentiality.[59]

---

[55] BEAUCHAMP & CHILDRESS, *supra* note 6, at 145–50.

[56] Robert M. Veatch, *Abandoning Informed Consent*, 25 HASTINGS CTR. REP. 5, 5 (Mar./Apr. 1995) ("Consent may be what can be called a transition concept, one that appears on the scene as an apparently progressive innovation, but after a period of experience turns out to be only useful as a transition to a more thoroughly revisionary conceptual framework.").

[57] *See, e.g.*, Berger v. Sonneland, 26 P.3d 257, 259 (Wash. 2001) (describing lawsuit where doctor discussed confidential information to patient's husband); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999) (concerning tort action for hospital's breach of patient's confidential but non-medical information); Hurvitz v. Hoefflin, 101 Cal. Rptr. 2d 558, 561 (Cal. Ct. App. 2000) (determining whether names of third party patients could be disclosed); Jeffrey H. v. Imai, Tadlock & Keeney, 101 Cal. Rptr. 2d 916, 918-19 (Cal. Ct. App. 2000) (outlining lawsuit for copying and disclosing confidential information on patient's medical status); McCormick v. England, 494 S.E.2d 431, 432 (S.C. Ct. App. 1997) (detailing patient's action against physician for breaching duty of confidentiality); Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 335 (N.Y. App. Div. 2001) (involving class action for purchase and sale of CVS's customers' medical and prescription information without authorization).

[58] *See, e.g.* Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972) (reversing District Court's directed verdict for doctor that failed to obtain informed consent from patient); Cobbs v. Grant, 502 P.2d 1, 7-12 (Cal. 1972) (setting forth jury instructions on informed consent and a doctor's duty).

[59] Humphers v. First Interstate Bank of Or., 684 P.2d 581, 587 (Or. Ct. App. 1984), *aff'd in part, rev'd in part*, 696 P.2d 527 (Or. 1985); *see also* Duquette v. Maricopa, 778 P.2d 634, 640 (Ariz. Ct. App. 1989) ("[T]he public has a widespread belief that information given to a physician in confidence will not be disclosed to third parties absent legal compulsion, and we further believe that the public has a right to have this expectation realized.").

Outside of such private law constructs federal constitutional protections for privacy have been relatively slow to develop,[60] although a small number of states have specific constitutional protections that use rights-based language in the context of privacy, and some of these constitutional provisions have been applied with rigor in healthcare cases.[61]

Congress adopted what was promulgated as the HIPAA-EDI model of health transactions in order to reduce the "back-end," transactional costs of healthcare delivery. That mandate was accompanied by powers to promulgate protective standards not because of a principled commitment to patient privacy or confidentiality but to minimize objections to and maximize participation in a transactional model desired by industry and promoted by government.

Instrumental fingerprints are all over the federal standards. As originally promulgated, the standards required that patients should consent to disclosure for treatment, payment, or healthcare operations (TPO) purposes.[62] Yet, the Bush administration amended the regulation, removing the requirement for consent[63] and replaced it with the permissive statement that "[a] covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations."[64] Of course, the original regulation provided little meaningful protection for patients; for example, the required consent could be general and the provider could refuse to treat a patient who refuses consent.[65] However, the value of that initial permission was educational and empowering; it offered a symbolic

---

[60] *But see* Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998) (holding that research institution violated federal privacy rights of clerical and administrative workers who were tested for intimate medical conditions without their knowledge as part of an employee health examination). *See also* U.S. v. Westinghouse Elec. Corp., 638 F.2d 570, 580 (3rd Cir. 1980) (holding that employee medical records fall within protected zone of privacy); U.S. v. Sutherland, 143 F. Supp. 2d 609, 610 (W.D. Va. 2001) (holding that government cannot disclose prescription records without giving patients a chance to object).

[61] *See, e.g.* In re Guardianship of Browning, 568 So. 2d 4, 10-12 (Fla. 1990) (discussing FLA. CONST. art. I, para. 23); *see also* King v. State, 535 S.E.2d 492, 494 (Ga. 2000) (discussing GA. CONST. art. I, § 1, para. 1). *But see* Rollins v. Ulmer, 15 P.3d 749, 750 (Alaska 2001) (finding that the registration requirements of Alaska's medical marijuana law were constitutional). *See also* Nicolas P. Terry & Leslie P. Francis, *Ensuring The Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 710-11 (detailing the U.S. constitution and Supreme Court's treatment of the right of privacy).

[62] 45 C.F.R. § 164.506 (2001), *amended by* 45 C.F.R. § 164.506 (2009).

[63] *See* 45 C.F.R. § 164.506(a) (2009).

[64] 45 C.F.R. § 164.506(b)(1) (2009).

[65] 45 C.F.R. § 164.506(b) (2001), *amended by* 45 C.F.R. § 164.506(b) (2009).

privacy–confidentiality "moment" that conveyed a "rights" message in much the same way that the requirement of consent to procedures asserts the precedence of autonomy over paternalism.

The adoption of an almost exclusively instrumental approach is further evidenced by the federal government's choice of enforcement models. The federal standards (in common with the majority of state standards on which they are modeled)[66] do not provide an aggrieved patient with enforcement through a private right of action; rather they provide for a compliance mechanism with regulatory agency oversight and the potential for civil or criminal penalties.[67] The message is that any privacy-confidentiality "rights" belong to the healthcare system and not to patients.

The use of instrumental rationales for patient privacy and confidentiality likely will be increased as systems are introduced to reduce medical error. Process-driven, technologically enabled healthcare delivery will tend to minimize the role of the individual autonomous physician (and the correlate autonomous patient), replacing autonomy and choice with systems that identify and potentially commoditize patients (e.g., by positively identifying them with bar codes) and reducing discretion in treatment (e.g., by relying on Clinical Practice Guidelines and Clinical Decision Support Systems). Such technologies have a huge, potentially deleterious impact on individuals' privacy and confidentiality. Yet, they are likely to be accompanied by minimalist protections that, as with the federal standards in HIPAA, will be designed so as not to impede the overall error-reducing model, for example, by favoring outcomes research to further the greater good of population-based care.

Just as so many courts have moved informed consent away from autonomy and back towards a type of quasi-paternalism (limiting its applicability by fact-pattern[68] and using professional custom as its standard),[69] so the federal standards have gutted the

---

[66] *See supra* text accompanying note 24 (pointing out lack of private right of action under state standards).

[67] Of course, some courts will "patch" this omission by back-filling a tort remedy modeled on statutory breach or informed by breach of the federal standards. *See, e.g.*, U.S. v. Sutherland, 143 F. Supp. 2d 609, 611-12 (W.D. Va. 2001) (comparing state and federal privacy laws); Doe v. Cmty. Health Plan-Kaiser Corp., 709 N.Y.S.2d 215, 216 (N.Y. App. Div. 2000) (alleging counts of negligence for disclosure of information).

[68] *See supra* note 54.

[69] *See, e.g.*, Campbell v. Palmer, 568 A.2d 1064, 1067 (Conn. App. Ct. 1990) (noting standards physician must follow). This "professional standards" or custom-based approach represents judicial backsliding from the patient expectations, autonomy-based approach of seminal cases such as *Canterbury v. Spence*, 464 F.2d 772 (D.C. Cir. 1972). *See generally* Ketchup v. Howard, 543

nascent rights-based approach to privacy and confidentiality, preferring an instrumental rationale that is almost totally focused on institutions and compliance.

IV. Distortions of the Physician–Patient Touchstone

When medicine's professional hegemony was at its most dominant in the legal domain, described by Rand Rosenblatt as a model designed to "support the authority and autonomy of individual physicians engaged in the practice of medicine,"[70] it was supportive of professional rather than patient autonomy. In more modern times and even as this core commitment was deconstructed by the courts and ethicists,[71] the physician–patient relationship has continued to play a dominant role in shaping, but ultimately distorting, our privacy-confidentiality model.

As a legal construct, the "physician–patient relationship" was important in the development of confidentiality-based restraints but ultimately corrosive of any broader sense of health privacy. First, the physician–patient relationship paradigm has favored the development of confidentiality rather than privacy models. Second, as the myriad of new relationships and structures that we collectively think of as industrialized medicine took hold (and as market theory began to dominate health regulation),[72] the traditional professional model had been reduced to a primarily operational concept with little or nothing to protect patient information. As a result and as healthcare delivery metamorphosed, industrial providers, who faced few ethical or legal constraints, began to exploit patient information for utilitarian or outright commercial purposes.[73] This negative process can be seen as the product of how the physician–patient relationship developed in overlapping domains and the increasingly fragmented care offered by modern delivery systems.

S.E.2d 371, 381-86 (Ga. Ct. App. 2000) (appendix providing a summary of different jurisdictions' approaches to the standard of disclosure).

[70] Rand E. Rosenblatt, *The Four Ages of Health Law*, 14 HEALTH MATRIX 155, 162–66 (2004) (describing the years of 1880 to 1960 as those in which the professional model dominated).

[71] *See id.* at 168–69.

[72] *See id.* at 175–90.

[73] The trend continues today. *See* Nicolas P. Terry, *Legal Barriers to Realizing the Public Good in Clinical Data*, *in* INSTITUTE OF MEDICINE, CLINICAL DATA AS THE BASIC STAPLE OF HEALTH LEARNING: CREATING AND PROTECTING A PUBLIC GOOD, Eds. (National Institutes of Health, forthcoming 2009) [hereinafter *Public Good in Clinical Data*]. *See generally* text accompanying note 88 (discussing apparent AMA interest in monetizing patient data).

A. Overlapping Domains and a "Race to the Bottom"

As an ethical construct the physician–patient relationship is neither monolithic nor singular. Different interpretations or models of the relationship have ranged from those that emphasize paternalism or friendship to the merely technical ("plumber"), amongst several metaphors.[74] Notwithstanding, it is the foundation of competence, respect, and confidence.[75] Thus, the ethical principles provide that, "[t]he patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest."[76]

In the legal domain, the "physician–patient relationship" synopsizes the contractual responsibilities of the parties (such as beginning and end, terms of service and payment), limits the physician's externalization of patient-incurred treatment or informational risks,[77] and defines and delimits various tort or fiduciary-based legal prescriptions ("duties").[78] The transposition of this professional (or ethical) paradigm into legal doctrine did much to preserve medicine's professional hegemony. For example, in the quality domain, it has been used to limit physician duties, impose internal professional standards (as dispositive of quality questions), and demote the importance of institutional responsibility.[79] Compared to the nuanced explication of the ethical domain, the legal domain's use of the physician–patient relationship has been far simpler, essentially contractual in its metaphor, and paternalistic in its policy. Crucially, given the simple delivery model of the physician–patient relationship, confidence arguably sufficed and any broader sense of legal protection of medical privacy was

---

[74] *See* James F. Childress & Mark Siegler, *Metaphors and Models of Doctor–Patient Relationships: Their Implications for Autonomy*, 5 THEORETICAL MED. & BIOETHICS 17, 17-21 (1984) (outlining various metaphors used in doctor-patient relationship).

[75] *See, e.g.*, American Medical Association, Principles of Medical Ethics (2001), http://www.ama-assn.org/ama/pub/category/2512.html (last visited Feb. 28, 2008).

[76] FUNDAMENTAL ELEMENTS, *supra* note 16, at para. 4.

[77] *See, e.g.*, Gray v. Grunnagle, 223 A.2d 663, 667-69 (Pa. 1966) (dealing with issue of consent during internal procedures where patient is under anesthesia).

[78] *See, e.g.*, Sterling v. Johns Hopkins Hosp., 802 A.2d 440, 444-59 (Md. Ct. Spec. App. 2002) (determining no duty of care thus no negligence); Kruger v. Jennings, No. 227480, 2002 WL 652098, at *3 (Mich. Ct. App. Apr. 19, 2002) (deciding doctor-patient relationship existed).

[79] *See generally* Nicolas P. Terry, *Through an E-Health Lens, Darkly: Observations on Law, Industry, and Innovation in Medicine and Industry*, *in* CHANGING PARADIGMS IN HEALTH LAW, POLICY AND ETHICS (George F. Tomossy et al. eds.) (forthcoming); Nicolas P. Terry, *A Medical Ghost in the E-Health Machine,* 14 HEALTH MATRIX 225, 225-26 (2004) (using e-health as a vehicle to portray this situation).

stillborn.

In the operational domain, the physician–patient relationship became synonymous with a simpler model, an ongoing relationship of care and treatment. This concept of "continuity of care" did not denote permanence but was founded on more than, say, the opportunistic prescribing relationship that a patient would have with a physician prescribing drugs on the Internet.[80] It was not a sophisticated state; rather, it identified the parties, denoted access to the patient's history, and highlighted purely operational requirements such as updating records. Instrumental justifications for medical confidence flourished in this operational domain. As already noted, "confidentiality" in this domain has tended to rotate around two co-dependent, practical imperatives: patients disclosing information to physicians to seek protection of their health and physicians respecting confidences in order to encourage patients to disclose needed personal and medical information.

In traditional, pre-industrial medicine, these three domains, ethical, legal, and operational, were essentially synchronized. In context, the parallelism between legal, ethical, and operational domains was not particularly harmful. The physician–patient relationship was not forced to deal with competition or conflict between the domains. But, as a practical matter, patient confidentiality was respected even though the rationale may have been instrumental and the model somewhat paternalistic. Over time, however, I believe that physicians, while cognizant and respectful of the ethical domain (albeit not particularly troubled by nascent legal rules on confidentiality), have primarily viewed confidentiality as a function or property of the operational domain. There was a slide to the lowest common denominator as the practical imperatives of the physician–patient relationship operation overshadowed and ultimately diminished the contributions of the ethical and legal domains. Consider, by way of example, how the AMA's Council on Ethical and Judicial Affairs (CEJA) undercuts its policy on confidentiality—"[t]he information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree"—with the instrumental observation that "[t]he patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services."[81]

---

[80] *See* Nicolas P. Terry, *Prescriptions sans Frontières (or How I Stopped Worrying about Viagra on the Web but Grew Concerned about the Future of Healthcare Delivery)*, 4 YALE J. HEALTH POL'Y L. & ETHICS 183, 188, 251 (2004) [hereinafter *Prescriptions sans Frontières*] (describing impact Internet has on doctor-patient relationship).

[81] *Id.*

By the time that the physician–patient relationship was replaced as the dominant delivery paradigm, little was left but operationally derived instrumental values. Legal conceptions of confidence and privacy were limited or underdeveloped, while the dominant instrumental values were ill prepared for a transition to new models of care.

B. The Ascendancy of Fragmented Care

The reasons cited to explain the decline of the physician–patient relationships are legion. Over two decades ago James Childress and Mark Siegler explained this phenomenon as follows:

> Numerous causes can be identified: First, the pluralistic nature of our society; second, the decline of close, intimate contact over time among professionals and patients and their families; third, the decline of contact with the "whole person," who is now parceled out to various specialists; fourth, the growth of large, impersonal, bureaucratically structured institutions of care, in which there is discontinuity of care. . . .[82]

To this catalogue we can add the growth of managed care (not to mention its potential for conflicts of interest and the vertical and horizontal integration it encouraged), an increase in the use of ambulatory care (which is episodic in nature and less stable as to its location), and the insertion of "new" players into the medical industrial complex, such as government rationing care, pharmaceutical companies seeking direct relationships with patients, and "docs-in-a-box" in retail stores,[83] web medical advice sites[84] and online pharmacies[85] ignoring traditional channels. Interestingly, perhaps even ironically, a very similar catalogue (the emergence of managed care, the rise of ambulatory care, and the horizontal and vertical integration of providers into delivery systems) today is used to explain the emergence of

---

[82] Childress & Siegler, *supra* note 74, at 22.

[83] *See, e.g.,* Press Release, Wal-Mart, 400 Health Clinics to Open in Wal-Mart Stores During Next Three Years, Up to 2,000 Could Open Over Next Five to Seven Years, (April 24, 2007), http://walmartstores.com/FactsNews/NewsRoom/6419.aspx (last visited Dec. 28, 2008) (announcing opening of health clinics within retail stores).

[84] *See generally* Nicolas P. Terry, *Cyber-Malpractice: Legal Exposure for Cyber-medicine*, 25 AM. J.L. & MED. 327, 349-58 (1999) (discussing different models of medical advice sites and legal implications).

[85] *See generally Prescriptions sans Frontières, supra* note 80, at 183-84 (outlining policy and legal implications of Internet prescribing).

technologically mediated care, particularly Electronic Health Records (EHR) systems.[86] These developments bring with them their own problems, as discussed below.[87]

Many of these changes, particularly the emergence of "shared care" (denoting that a patient should share responsibility with his or her provider for care)[88] may be viewed as potentially beneficial and the beginning of a new contracting model of autonomy between rational actors involved in healthcare. In the interim, however, they point to a new healthcare delivery paradigm with primarily negative short-term implications—fragmented care delivered in a medico-industrial setting.

Ethicists have long recognized the deterioration of the traditional physician–patient relationship, and its regrettable shift from a relationship of intimates to encounters between strangers. As Childress and Siegler noted:

> Whether medicine is now only a series of encounters between strangers rather than intimates, medicine is increasingly regarded by patients and doctors, and by analysts of the profession—such as philosophers, lawyers, and sociologists—as a practice that is best understood and regulated as if it were a practice among strangers rather than among intimates.[89]

A concept of privacy-confidentiality protection that is bound to an outdated conception of the confidence inherent in a single physician–patient relationship was bound to fail when the physician–patient relationship was replaced by fragmented care. Domain synchronization evaporated, and it is unlikely that patients comprehended the extent of their "agreement" to disclose given the institutional settings within which their

---

[86] *See, e.g.*, Paul C. Tang & W. Ed Hammond, *A Progress Report on Computer-based Patient Records in the United States*, in THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE 1 (D.E. Detmer et al. eds., rev. ed. 1997); Tracy D. Gunter & Nicolas P. Terry, *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*, 7 J. MED. INTERNET RES. e3 (2005), http://www.jmir.org/2005/1/e3 (providing description of EHR, different EHR models, and practical and legal challenges of EHR).

[87] *See infra* text accompanying note 93, *et seq.* (explaining technology creates issues that ethic and legal constructs have failed to discuss).

[88] *See, e.g.* Peter Briss et al., *Promoting Informed Decisions About Cancer Screening in Communities and Healthcare Systems*, 26 AM. J. PREVENTIVE MED. 67, 67 (2004) (defining shared decision making, noting its importance, but realizing that it alone is not enough to elicit informed decision making).

[89] Childress & Siegler, *supra* note 74, at 22.

information was destined to circulate.[90] Equally, patients are unlikely to understand the level of information processing, such as commercial aggregation,[91] that such settings employ or facilitate. At a time of uncertainty (and, specifically, informational asymmetry), it was hopeful that the legal domain would operate as a corrective, by supplying "rights." As already noted, however, the legal domain failed to develop meaningful privacy protections and a rights-based approach to breach of confidence was slow to develop.[92] Breach of confidence was far slower to develop, for example, than informed consent, its autonomy-based fellow traveler. This legal vacuum created the opportunity for the federal standards. Unfortunately, this opportunity came in an atmosphere that by now stressed operational (and hence instrumental) goals rather than the broad principles reflected in ethical or legal rights-based approaches.

V. Healthcare Information: Another Domain Unfolds

It is too early to assess the final impact of the ongoing healthcare technology revolution but, inevitably, aspects of the delivery system will be fundamentally changed. Two key sets of technologies are at issue here. The first can be viewed as disruptive—technologies that replace traditional methods of delivery. These include web-based medical content, online consultations, and Internet-prescribing. The second is more integrative—the leveraging of information technologies (IT) by traditional healthcare providers to improve the quality of care and reduce its cost structure. Both sets bring with them difficult privacy issues. Thus, disruptive technologies, in large part because of their novelty, tend to create issues that our ethical and legal constructs have generally failed to address.[93] For example, non-traditional providers, such as those engaged in Internet advice or prescribing generally are not covered by disclosure-centric confidentiality regulation.[94]

---

[90] BEAUCHAMP & CHILDRESS, *supra* note 6, at 419–20.

[91] *See, e.g.*,, Regina v. Dep't of Health, [2001] Q.B. 424, 425-27 (information aggregator seeking to collect information about physician prescribing habits and sell data to pharmaceutical companies challenged U.K. policy prohibiting same); *see also* In re Pharmatrak, Inc., 292 F. Supp. 2d 263, 265 (D. Mass. 2003) (class action against information aggregator and pharmaceutical companies, alleging that they intercepted and accessed Plaintiffs' personal information through the use of computer "cookies" and other devices, in violation of state and federal law).

[92] *See supra* note 20, *et seq.*

[93] *See generally Prescriptions sans Frontières, supra* note 80 (delineating various issues that arise with Internet prescribing and dispensing).

[94] *See generally id.* at 244 (comparing traditional and non-traditional providers coverage under the disclosure-centric confidentiality regulation).

A. Healthcare Technologies

The second cluster of technologies particularly highlights privacy and confidentiality issues as traditional providers increasingly adopt IT models. In pre-industrial, pre-IT medicine, patient-specific health data was proprietary and non-integrated. Physicians owned their patients' data (both health and billing information)[95] and as a result, data collection models were inconsistent, the data itself was incomplete, and storage was fragmented across the information silos of multiple providers. In contrast, information technologies are built on the premise that processes are improved (both as to outcomes and process efficiencies) by maximizing the collection of information, consolidating or linking information silos (creating longitudinal patient data), and making the information available to multiple users in comparable form and through common and consistent interfaces. U.S. healthcare is in the throes of a fundamental transition to IT-dominated models for healthcare transactions, risk-management, and record keeping.

As already noted, HIPAA's "Administrative Simplification" seeks to improve "the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." To reduce "back-end" costs associated with billing, reimbursement, eligibility inquiries, insurance claims, and prescription fulfillment,[96] HIPAA adopted the e-commerce model of Electronic Data Interchange (EDI)—the electronic exchange of standardized business documents (or messages) between "trading partners." The HIPAA-EDI requires healthcare-specific data standards:[97] unique identifiers for health-care providers, health plans, employers, and patients;[98] specific message formats for healthcare transactions

---

[95] *See, e.g.*, Breen v. Williams (1996) 186 C.L.R 71, 80 (Austl.) ("Documents prepared by a professional person to assist the professional to perform his or her professional duties are not the property of the lay client; they remain the property of the professional.").

[96] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L No. 104–91, § 261, 110 Stat. 1936 (1996) (detailing purpose of legislation); *see also* S.C. Med. Ass'n v. Thompson, 327 F.3d 346, 348 (4th Cir. 2003) ("HIPAA's Administrative Simplification provisions . . . were designed to improve the efficiency and effectiveness of the health care system by facilitating the exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information in connection with such transactions.").

[97] *See generally* Office of the Assistant Secretary for Planning and Evaluation, Administrative Simplification in the Health Care Industry, http://aspe.hhs.gov/admnsimp/index.shtml (last visited Dec. 13, 2008) (providing links to various standards).

[98] *See generally* Centers for Medicare and Medicaid Services, HIPAA General Information-

such as enrollment, eligibility, payment and remittance advice, claims, health plan premium payments, health claim status, and referral certification and authorization;[99] transaction codes (for example, benefit denial or additional information requested) that are used within the messages; and common formats for healthcare claims attachments (such as excerpts from medical records) and information about diagnoses and treatment.

The publication of major national studies of medical error rates[100] has led to broad calls for amelioratory systems or process redesign of healthcare delivery.[101] The resultant, and now rapid, massive infusion of technology into healthcare is a key component in process-based reform.[102] This IT-led system reform is centered on several intersecting technologies. "Tracking" or identifying technologies such as barcodes and Radio Frequency Identification (RFID) positively identify drugs, dosages, and patients.[103] "Entry" technologies consist of computerized physician order entry (CPOE) systems that seek to avoid medication errors caused by illegibility and other recording mistakes.[104] Clinical Decision Support Systems (CDSS)[105] are evolved order entry systems that have lost their passivity and reference drug interaction information, EHR data, or treatment models (such as clinical practice guidelines), and which offer

---

Overview, http://www.cms.hhs.gov/hipaaGenInfo/ (last visited Dec. 13, 2008) (providing information on standards created as require by HIPPA).

[99] *See* Centers for Medicare and Medicaid Services, Transaction and Code Sets Standards-Overview, http://www.cms.hhs.gov/TransactionCodeSetsStands/ (last accessed Dec. 13, 2008) (providing links for standards on transactions).

[100] COMMITTEE ON QUALITY OF HEALTH CARE IN AMERICA, IOM, TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM (Linda T. Kohn et al. eds, 1999); Chunliu Zhan & Marlene R. Miller, *Excess Length of Stay, Charges, and Mortality Attributable to Medical Injuries during Hospitalization*, 290 JAMA 1868 (2003).

[101] *See generally* Lucian L. Leape, *Preventing Medical Accidents: Is "Systems Analysis" the Answer?*, 27 AM. J.L. & MED. 145, 145-48 (2001) (discussing reasons and impact of the report *To Err is Human*); James Reason, *Human Error: Models and Management*, 320 BRIT. MED. J. 768, 768f (2000) (differentiating between person and system approach in human error and implications differences have in overall human error problem).

[102] COMMITTEE ON QUALITY OF HEALTH CARE IN AMERICA, IOM, CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY 15 (2001) (describing potential Internet has for health care).

[103] *See generally* 21 C.F.R. §§ 201, 606, 610 (2004) (addressing new rule on bar codes).

[104] *See* PETER KILBRIDGE, E-PRESCRIBING 11 (2001), *available at* http://www.chcf.org/documents/hospitals/EPrescribing.pdf (last accessed Dec. 13, 2008) (noting example of how General Motors is working to reduce recording mistakes).

[105] *See generally* Rainu Kaushal & David W. Bates, *Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs), in* MAKING HEALTH CARE SAFER: A CRITICAL ANALYSIS OF PATIENT SAFETY PRACTICES 59 (2001), *available at* http://www.ahrq.gov/clinic/ptsafety/pdf/ptsafety.pdf (last visited Sept. 20, 2001) (describing and promoting CPOEs).

considerable advantages over simple CPOE systems.[106] "Reporting" systems provide for adverse event and medical error disclosure and reporting,[107] and facilitate population-based healthcare models and outcomes research.[108]

President Clinton's HIPAA-EDI may have been the first major federal e-health initiative with serious implications for medical information privacy and confidentiality, but it was not the last. President George W. Bush's administration took its own first steps into e-health by authorizing DHHS to develop e-prescribing standards under the *Medicare Modernization Act of 2003*,[109] in part to offset the costs of the Part D prescription drug benefit. Even today some components of the transactional and e-prescribing systems continue to struggle towards full implementation.[110]

On April 26, 2004, President Bush announced his goal of assuring that most Americans will have electronic health records within the next ten years.[111] To this end, the President appointed a National Health Information Technology Coordinator to guide the "nationwide implementation of interoperable health information

---

[106] *See, e.g.,* Anne Bobb et al., *The Epidemiology of Prescribing Errors: The Potential Impact of Computerized Prescriber Order Entry*, 164 ARCHIVES INTERNAL MED. 785 (2004) (noting the desirability of matching CPOE systems to decision support and pharmacy systems to reduce medication errors). *See* Bernard Fernando et al., *Prescribing Safety Features of General Practice Computer Systems: Evaluation Using Simulated Test Cases*, 328 BRIT. MED. J. 1171, 1171 (2004) (studying four main computer systems in United Kingdom).

[107] *See, e.g.*, AUSTRALIAN COUNCIL FOR SAFETY AND QUALITY IN HEALTH CARE, OPEN DISCLOSURE: A NATIONAL STANDARD FOR OPEN COMMUNICATION IN PUBLIC AND PRIVATE HOSPITALS FOLLOWING AN ADVERSE EVENT IN HEALTH CARE (July 2003), *available at* http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/F22384CCE74A9F01CA257483000D845E/$File/OpenDisclosure_web.pdf (last visited Dec. 13, 2008).

[108] *See generally* Agency for Healthcare Research and Quality, Outcomes & Effectiveness, http://www.ahrq.gov/clinic/outcomix.htm (last visited Dec. 13, 2008).

[109] Medicare Modernization Act of 2003, Pub. L. No. 108-173 § 1201, 117 Stat. 2066 (codified in scattered sections of 42 U.S.C.).

[110] *See, e.g.*, CENTERS FOR MEDICARE & MEDICAID SERVICES, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, GUIDANCE ON COMPLIANCE WITH THE HIPAA NATIONAL PROVIDER IDENTIFIER (NPI) RULE AFTER THE MAY 23, 2007, IMPLEMENTATION DEADLINE, www.cms.hhs.gov/NationalProvIdentStand/Downloads/NPI_Contingency.pdf (last visited Dec. 13, 2008) (providing for "good faith" relaxed enforcement of sanctions for non-compliance with National Provider Identifier deadline); Joy M. Grossman et al., *Physicians' Experiences Using Commercial E-Prescribing Systems*, HEALTH AFFAIRS, Apr. 3, 2007, http://content.healthaffairs.org/cgi/content/full/26/3/w393.

[111] *Bush Proposes Update of Medical Records*, FOX NEWS, Apr. 27, 2004, http://www.foxnews.com/story/0,2933,118330,00.html.

technology."[112] The EHR is a database record that incorporates a patient's healthcare details from conception to death (i.e., it is longitudinal) and can be distributed over a number of sites or aggregated at a particular source.[113] It is a core technology promoted by the patient-safety movement in large part because it will provide much-needed cohesion for decision-support systems, error reporting, and outcomes research.[114]

B. Managing Privacy in the Health Information Domain

In pre-IT times and consistent with an operational paradigm of fragmented record-keeping, the legal protection of patient data was achieved principally through a physician–patient relationship disclosure-centric rule, expressed as breach of confidence and operationalized through implied contract or torts doctrine. Even given the relative weakness of the disclosure-centric confidentiality model or assuming its occasional breach, patient "privacy" was somewhat protected by the sheer inefficiencies of a system built around unstructured, distributed patient data.

This paradigm has now been overwhelmed by the realities of the modern health information domain. The patient data contained in modern longitudinal systems is comprehensive, portable, and manipulatable. The potential for abuse is immense; there are many parties (pharmaceutical companies and government being the obvious examples, inquisitive healthcare employees being the most commonly reported[115]) that crave access to this data. As a result, the privacy and confidentiality costs potentially incurred by patients rise exponentially.[116]

The emerging health information domain has several key properties that extend beyond the confidentiality inherent in the physician–patient relationship.[117] In addition to the confidentiality–privacy–anonymity triumvirate that protects (or should protect) the basic input and output of patient data, the contemporary health information domain has (or should possess) several additional properties (or qualities). These protective rules give rise to "process" controls such as "security" (a confidentiality correlate that

---

[112] Exec. Order No. 13,335, 69 Fed. Reg. 24059 (April 27, 2004).

[113] Nicolas P. Terry, *Electronic Health Records: International, Structural, and Legal Perspectives,* 12 J.L. & MED. (AU) 26 (2004) [hereinafter *Structural and Legal Perspectives*].

[114] *Id. See also* Nicolas P. Terry, *To HIPAA, A Son: Assessing the Technical, Conceptual, and Legal Frameworks for Patient Safety Information*, 12 WIDENER L. REV. 134 (2006).

[115] *See, e.g.,* Andrew Blankstein, *Digging into celebrity medical records has a long history*, L.A. TIMES, May 19, 2008, http://articles.latimes.com/2008/may/19/local/me-tabs20.

[116] *See generally* Terry & Francis, *supra* note 61.

[117] *See generally Health Information Domain, supra* note 5.

restricts access to data to those authorized to receive it) and "integrity" (data "checksum" validation and protection against unauthorized modification). As data is aggregated, additional properties such as "unity," "quality," and "accountability" become paramount because information domains lose their value proposition when they are incomplete or their data is otherwise flawed. "Unity" refers to health information that is "longitudinal," consisting of records from various providers that are consolidated or interlinked to provide a comprehensive view of a patient's healthcare encounters. A longitudinal approach provides the data necessary to interface with other technologies (such as CDSS) that analyze diagnoses and treatments and support shared care from multiple providers. "Quality" denotes that the data must be current or timely and subject to quality auditing from extrinsic sources such as clinical practice guidelines. Finally, the "accountability" property denotes not only substantive responsibility by providers for the accuracy of the data they enter but also procedural identification of providers responsible for specific data.

The modern health information domain must also take into account and integrate the increasing demands for access to the data it contains. Thus, the "access" property describes the various recognized claims to view and, in some cases, modify patient information. Justice and public health systems make the most persistent claims. However, most mature health information domains also recognize patients' rights of access and correction of their own data. Outcomes assessment and error-reporting mandates will substantially increase demands for access to individual and population-based health records from accreditation bodies and government regulators.[118]

What the discussions of privacy and confidentiality in the context of transaction standards, error reduction, and electronic health records have in common is a heavily instrumental approach to health information. This is because the IT revolution that has brought about the health information domain has less to do with improving or increasing patient access to services and more with business imperatives. Such imperatives include reducing healthcare transaction costs (the expenses associated with medical errors), the inefficiencies associated with multiple providers, and changing roles of physicians in a managed care environment.[119] As a result, individual autonomy tends to be viewed as subordinate to broader goals (e.g., lower costs and a reduction in medical errors) that may or may not directly benefit the individual involved.

When it came time (during the HIPAA debate) to force providers to internalize

---

[118] *See generally Public Good in Clinical Data, supra* note 73.

[119] *See generally* Terry, *supra* note 79.

some of the privacy risks associated with new technologies, it was perhaps inevitable that federal architects would eschew traditional "rights" approaches and strike a new direction. After all, and as already discussed,[120] the physician–patient relationship model of privacy-confidentiality protection had become operational rather than principled, and the common law models were unsophisticated and underdeveloped. There is every indication that any new privacy protections that are clustered around the emerging EHR model will adopt a similar style and correspondingly lower the level of protection.

Indeed, one of the four cornerstones of the national EHR initiative identified by Dr. David Brailer, President Bush's first National Coordinator was to address "variations in privacy and security policies that can hinder interoperability."[121] As noted elsewhere[122] the national EHR "insiders" viewed this as a mandate to replace the HIPAA "floor," whereby more stringent state privacy protections are not preempted,[123] with something more akin to a HIPAA "ceiling," tipping the balance away from patient PCS protections in order to facilitate the national EHR.

It does not have to be this way. For example, the Australian EHR experiment, known as HealthConnect,[124] eschewed utilitarianism for models clearly based on a "contracting" autonomy model. HealthConnect, before its effective demise by 2006[125] was a "push" system, selectively sending data to a centralized record, and the patient controls which elements of the centralized record may be used for what purposes or displayed in which "views."[126] The Australian model did not create a comprehensive longitudinal record. Rather, patients, with their providers, choose which elements may be extracted from an existing health record and transferred to their separate but centralized HealthConnect record.

---

[120] *See supra* note 74, *et seq.*

[121] *Activities of the Office of the National Coordinator for Health Information Technology: Testimony before the S. Comm. on Commerce, Science, and Transportation Subcomm. on Technology, Innovation, and Competitiveness*, 109th Cong. (2005) (statement of David J. Brailer, M.D., Ph.D., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services) http://www.hhs.gov/asl/testify/t050630a.html [hereinafter *Brailer Testimony*].

[122] Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?* DREXEL U. L. REV. (forthcoming 2009). *See supra* text accompanying notes 161-164.

[123] 45 C.F.R. § 160.202 (2009).

[124] *See* HealthConnect archive, http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/home (last visited Jan, 26, 2009).

[125] *See* Department of Health and Ageing, Health Connect, http://www.health.gov.au/internet/main/publishing.nsf/Content/EHeath+Healthconnect (last visited Jan. 26, 2008).

[126] *See generally Structural and Legal Perspectives, supra* note 113, at 32.

In contrast, what is striking about the administrative standards and compliance mechanisms of the U.S. federal standards is the relatively low level of patient protection they contain; the complex regulations read more like a catalogue of exceptions than of rights.

VI. Professional Hegemony, Compliance, and Distrust

In the last few decades, healthcare's legal domain has experienced its most fundamental revolution; a change from profession-dominated medical boards and ex post facto torts regulation (based on professional standards) to regulatory systems that not only are frequently federal rather than state but also use a "command-control" approach. This regulation began as a way of pushing the health system during what Rand Rosenblatt has labeled the "egalitarian social contract" model of health law[127] and, thereafter, as a method of reducing market distortions in the same author's "market competition" model.[128] It represents a fundamental shift from hegemony to compliance-based legal regulation. Once confidentiality, courtesy of the federal standards, joined the regulatory matrix, it became a target for those who criticize the level and style of governmental regulation of healthcare.

A. Unsupportive Regulation

Mark Hall has provided one modern theoretical context for this battle over privacy and confidentiality. In an influential article, Hall has argued that "trust" can be an organizing principle (or at least a dominant theme) for health law.[129] He premises this "centrality" of trust on both instrumental ("Trust is the core, defining characteristic of the doctor–patient relationship – the 'glue' that holds the relationship together and makes it possible")[130] and therapeutic (both empirical and jurisprudential) grounds.[131]

Hall regards "trust" in healthcare as the Mary Tyler Moore Show viewed love in Minneapolis. Thus, "[trust] is all around, no need to waste it"[132] is the foundation for his contractarian attack on healthcare regulation.[133] Hall categorizes health law

---

[127] Rosenblatt, *supra* note 70, at 166–75.
[128] *Id.* at 175–90.
[129] Mark A. Hall, *Law, Medicine, and Trust*, 55 STAN. L. REV. 463, 464–66 (2002).
[130] *Id.* at 470.
[131] *Id.* at 479–82.
[132] SONNY CURTIS, LOVE IS ALL AROUND (Theme song to *Mary Tyler Show* 1970).
[133] *Accord* M. Gregg Bloche, *Trust and Betrayal in the Medical Marketplace*, 55 STAN. L. REV. 919, 922–26 (2002).

principles as predicated on, supportive of, or skeptical of trust.[134] In this matrix, Hall views confidentiality laws as attempts to support trust and argues they are unnecessary because of the existence of trust or because they frustrate the role of trust in promoting market approaches to securing the appropriate level of confidentiality and privacy.[135] Further, he views both the traditional common law of confidence and the federal standards as "explicitly premised on the therapeutic need to reassure patients that they can trust their physicians with sensitive, embarrassing, or even incriminating information, rather than on inherent rights arising from the mere expectation of privacy."[136]

As follows from the discussion above, Hall's description of modern health privacy-confidentiality law is partially correct; it is based on instrumental values rather than, say, autonomy.[137] However, that does not amount to an approval of such a theoretical basis. Further, the instrumental values displayed by the federal standards are not, as Hall states, "therapeutic" but far more utilitarian in character.[138] Greg Bloche meets Hall's approach head-on:

> A large body of scholarship and case law treats privacy as a right, important for personal dignity and psychological welfare. The law's protection for medical privacy follows from this more general right. Yet Hall disregards both the existence of this right and its grounding in the law's concern for citizens' dignity and mental well-being. . . . [A]ll that matters for Hall in evaluating the need for these (and other) legal protections for medical privacy is whether these safeguards do in fact promote trust. The actual protection these safeguards provide for citizens' privacy interests does not count within Hall's evaluative framework, since these interests, in themselves, are not part of his framework.[139]

Bloche's painting of Hall as a cardboard contractarian is tempting because of the latter's "over-selling" of "trust"; his trust hypothesis is just that, and he fails to provide convincing evidence or arguments that "trust" is more important, illuminating, or unifying than traditional ethical and legal underpinnings such as autonomy, rights-

---

[134] Hall, *supra* note 129, at 486.
[135] *Id.* at 504–6.
[136] *Id.* at 499.
[137] *See supra* note 40.
[138] *See supra* note 44, *et seq.*
[139] Bloche, *supra* note 133, at 940.

analysis, or social contract theories. Yet, "trust" is appealing. It is common to most of the positive metaphors that are used to explicate the physician–patient relationship (such as friendship and negotiation) and so is worthy of Hall's "glue" appellation. It is also a comforting aspiration, something that combines therapeutic soundness with the potential to rehabilitate some of the more corrosive states of the healthcare delivery system.

"Trust," however, is not a current state, and Hall's empirical evidence[140] may be premature because there is good reason to suspect growing patient distrust of healthcare providers. For example, a 2004 poll found that the reputations of pharmaceutical and health insurance companies continue to slide precipitously.[141] When asked specifically about the extent of their trust for healthcare providers, fifty-nine percent of Americans replied that they distrusted health insurers and forty-one percent distrusted pharmaceutical companies. While physicians and nurses fared better, some forty percent of those polled did not trust them "a lot."[142] Furthermore, patient concerns about the security and privacy of their health information continue to be significant in surveys measuring patient satisfaction in technologically mediated care.[143] Finally, his approach is fundamentally flawed in treating contemporary issues of health information privacy today as essentially similar to those in pre-IT healthcare. To the contrary, and as noted by architects of the United Kingdom's new health information system,

> [T]rust relating to the use of data needs to be earned. In practice this means health professionals need to understand current anxieties about the ways in which health information is handled; they need to learn the rules and apply them and accept that unfettered access to personal health information is a thing of the past and that, among the many

---

[140] Hall, *supra* note 129, at 473.

[141] Harris Interactive, *Reputations of Pharmaceutical and Health Insurance Companies Continue Their Downward Slide*, 4(11) HEALTHCARE NEWS 1, June 22, 2004, at 1, *available at* http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2004Vol4_Iss11.pdf. The same poll found the reputation of hospitals also declining but that they are generally well regarded, albeit ranked behind, for example, software companies and airlines.

[142] Harris Interactive, *Health-Care Professionals, Pharmacies, Hospitals Gain the Public's Top Trust,* 3(2) THE WALL STREET JOURNAL ONLINE/HARRIS INTERACTIVE HEALTH-CARE POLL 1, Jan. 28, 2004, at 1, http://www.harrisinteractive.com/news/newsletters/wsjhealthnews/WSJOnline_HI_Health-CarePoll2004vol3_iss02.pdf.

[143] *See, e.g.*, Christopher N. Sciamanna et al., *Patient Attitudes toward Using Computers to Improve Health Services Delivery*, 2(1) BMC HEALTH SERV. RES.19 (2002); Andrea Hassol et al., *Patient Experiences and Attitudes about Access to a Patient Electronic Healthcare Record and Linked Web Messaging*, 11(6) J. AM. MED. INFORMATICS ASSOC. 505 (2004).

> tools they need for modern clinical practice are those of skilled information management.[144]

Patients, physicians, and regulators alike are nervous and skeptical about the new demands placed on health information. Unfortunate and debilitating of the therapeutic relationship it may be, but today, it is *distrust* that is all around.

B. Limitations and Gaps

Hall classifies the federal standards within his matrix as attempts to be "supportive" of trust. More extreme anti-regulatory contractarians might view those same standards as attracting Hall's more damning categorization of a type of health law, as "skeptical of trust."[145] Market proponents should be able to argue that such information regulation imposes immense costs whose benefits have not been bargained for and distort healthcare markets by impeding provider–provider arrangements. Indeed, twenty years ago Richard Posner criticized "economically perverse legislative responses to privacy issues,"[146] arguing against a "trend toward elevating personal and downgrading organizational privacy."[147]

The transition to HIPAA-EDI and the federal standards has not been easy. Implementation woes continue, as a result of missing or delayed claims, non-standardized transactions, multiple party processing, and unsuccessful massaging by clearinghouses.[148] The AMA has even set up an online system to facilitate complaints.[149] Regarding privacy, there are frequent reports that the federal standards are impeding the delivery of healthcare,[150] and the United States Department of Health & Human Services (HHS) is continually updating its web site to answer detailed questions about

---

[144] Jim Chalmers & Rod Muir, *Patient Privacy and Confidentiality*, 326 BRIT. MED. J. 725 (2003) (discussing NHS Information Authority initiatives).

[145] Hall, *supra* note 129, at 512–24.

[146] Richard A. Posner, *An Economic Theory of Privacy, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 333, 344 (Ferdinand D. Schoeman ed., 1984).

[147] *Id.* at 343.

[148] Joel B. Finkelstein, *HIPAA's Promise Undermined by Claims-Processing Tangle*, AMNEWS, Sept. 13, 2004, http://www.ama-assn.org/amednews/2004/09/13/gvsa0913.htm.

[149] *HIPAA Complaint Form*, AM. MED. ASS'N, http://www.ama-assn.org/ama/pub/category/11132.html (last visited Jan. 28, 2009).

[150] *See, e.g.*, Ondria C. Gleason & William R. Yates, *Suicide Attempt Due to a Misunderstood HIPAA Notice*, 161 AM. J. PSYCHIATRY 374 (2004) (noting misinterpretation of privacy notice from insurer as notice of non-coverage, possibly contributing to suicide attempt).

the applicability of the privacy standards.[151] Even avid supporters of the federal standards would find it difficult to disagree with the scathing comments of Senator Larry Craig that "as is often the case with federal rulemaking, a kernel of congressional intent has grown into a towering tree of regulatory complexity. But even by federal bureaucratic standards, HIPAA is extraordinary."[152] Not surprisingly, some healthcare providers, although avowing support for patient confidentiality, have challenged the validity of the federal standards[153] with no more success than the medical privacy advocates who challenged the Bush administration amendments.[154]

In fact, there are some very real criticisms that should be aimed at the federal standards—not criticisms of regulatory inappropriateness but, rather, under-regulation and a level of complexity that diminish the educative value of the standards. The catalogue of HIPAA privacy blunders is large and that which follows is not an exhaustive list. First, the privacy architecture seems backwards; it concentrates almost exclusively on the process of patient consent to disclosure. A privacy regime should be more substantively concerned with limiting the collection and dissemination of personal health information. Only at the margins should questions of patient consent to disclosure need to be addressed. Further, as already detailed, the Bush administration removed an already weak consent-to-disclosure provision, thus, denying a privacy-autonomy "moment" at the commencement of the provider–patient relationship.[155] Second, although HIPAA confidentiality is premised on national standards, limitations in the enabling legislation prevented the inclusion of patient protective features extant in some state laws. Unwilling to detract from existing privacy protections, the drafters constructed a confusing and operationally obstructive "more stringent" partial preemption rule.[156] The result is that simply establishing the applicable standard of health privacy protection in a particular state requires complex (and ongoing) analysis.

---

[151] U.S. Dep't of Health and Human Serv., Health Information Privacy, http://www.hhs.gov/ocr/hipaa (last visited Jan. 28, 2009).

[152] *HIPAA Medical Privacy and Transactions Rules: Overkill or Overdue? Hearing Before the Spec. Comm. on Aging,* 108th Cong. 256 (2003) (statement of Senator Larry Craig), *available at* http://www.access.gpo.gov/congress/senate/pdf/108hrg/91119.pdf (last visited Jan. 28, 2009).

[153] *See, e.g.,* S.C. Med. Ass'n v. Thompson, 327 F.3d 346 (4th Cir. 2003), *cert. denied,* 540 U.S. 981 (2003) (physicians and medical association challenged federal privacy rule for vagueness and impermissible delegation). *See also* Ass'n of Am. Physicians & Surgs., Inc. v. United States Dep't of Health and Human Serv., 224 F. Supp. 2d 1115 (S.D. Tex. 2002).

[154] *See, e.g.*, Citizens for Health v. Thompson, No. 03-2267, 2004 U.S. Dist. LEXIS 5745 (E.D. Pa. Apr. 2, 2004) (court denied challenge to Bush administration amendment to the privacy rule, holding that the Secretary had examined the evidence and provided a reasoned analysis).

[155] *See supra* note 62, *et seq.*

[156] 45 C.F.R. § 160.202 (2009).

Third, and true to their instrumental rationale, the federal standards apply broad exceptions (public health, judicial, and regulatory) where patient consent to data processing is not required.[157] Fourth, the privacy standards are still too lax regarding secondary uses of patient information. There are still many unrestricted uses of patient information outside of treatment and billing; in too many situations patient consent for secondary uses is not required[158] and in other situations, consideration should have been given to prohibiting some consented-to secondary uses (e.g., the sale of patient data for pharmaceutical marketing).

Above all, the standards lack transparency and clarity. They may be labeled as promotional of "privacy" (in fact mislabeled because they deal only in confidentiality) but their sheer weight and obliqueness detracts from any educative or principled "message." With all the amendments, the combined privacy and security standards now consist of fifty-five pages of dense regulatory language.[159] By way of contrast, the Australian Health Privacy Principles, which provide far more protection of health information using both collection-centric and disclosure-centric models, take up a mere six pages of text.[160] What was required of the federal standards was a more generalized statement of principle based clearly on an autonomy-focused rationale; a legal guarantee that patients have control of their health information. Exceptions should have been far more narrowly constructed and tightly controlled by concepts of proportionality and relevance to medical and billing services.

The health insurance crises of the last three decades likely fueled the decision to omit a private right of action for breach of the federal standards. But, clearly stated rights and duties have an important educational value that is not captured by *pro forma* privacy notices, while caps on recovery (or other limitations) would have been a better tool to minimize litigation risks. A far better model would have been to appoint an independent, statutorily authorized patient privacy advocate, such as the Australian Federal Privacy Commissioner,[161] Ontario's Information & Privacy Commissioner,[162] or

---

157 45 C.F.R. § 164.512 (2009).

158 *See generally* 45 C.F.R. §§ 164.505, 164.508, 164.510 (2009).

159 U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, COMPLETE PRIVACY, SECURITY, AND ENFORCEMENT (PROCEDURAL) REGULATION TEXT (45 CFR PARTS 160 AND 164) (Aug. 2003).

160 OFFICE OF THE PRIVACY COMMISSIONER, PRIVATE SECTOR INFORMATION SHEET 1A – NATIONAL PRIVACY PRINCIPLES, http://www.privacy.gov.au/publications/npps01.pdf (last visited Jan. 28, 2009).

161 Office of the Federal Privacy Commissioner, Privacy Complaints, http://www.privacy.gov.au/privacy_rights/complaints/index.html (last visited Jan. 28, 2009).

162 Information and Privacy Commissioner of Ontario, http://www.ipc.on.ca (last visited Jan. 28,

the United Kingdom's Information Commissioner,[163] who could investigate consumer complaints, attempt to mediate disputes, and where necessary apply sanctions.

VII. Conclusion

Of course there are more problems with health privacy than detailed in this essay. As I have argued elsewhere, aggressive plaintiffs' lawyers likely will now add common law or *per se* styled breach of privacy allegations in medical error cases, just as duty to warn counts now routinely turn up in products liability actions and as informed consent counts are used to buttress lackluster surgical or medication error cases. Also, it is likely that plaintiffs will use any knowledge they have of provider non-compliance with the federal regulations—along with all of the penalty ramifications that brings—as leverage to negotiate a settlement in tangentially related malpractice cases.[164]

Admittedly, my litany of complaints about the state of health privacy and healthcare delivery is not entirely consistent. For example, I bemoan the decline of the physician–patient relationship because of its negative impact on the development of privacy, yet I welcome the breakdown of professional hegemony. While this essay may paint a dire picture of technologically mediated care impacting patient information, here and elsewhere I have been an advocate for technological models.

The goal here, however, is modest. To combine the normative and descriptive aspects of this essay's ambiguous title, if there's nothing wrong with health privacy why isn't it what it seems, why aren't its foundation stronger, why is it likely to get worse before it gets better, and why can't we explain the goals and basic principles of modern health privacy law to patients and providers in just a few sentences? The answers to those questions suggest to me that health privacy lies in a fragile state.

2009).

[163] Information Commissioner's Office, http://www.informationcommissioner.gov.uk (last visited Jan. 28, 2009).

[164] Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361, 385 (2001).